Entropy Amplification by Aperiodic Noise and Applications to Side Information Problems

Aaron S. Cohen
Brown University

Ram Zamir
Tel Aviv University

DIMACS Workshop on Algebraic Coding & Information Theory
DIMACS Center, Rutgers University
December 16, 2003
Outline

• Aperiodic Noise
  – Definition
  – Difference Set Noise – Maximal Aperiodic Noise
  – Entropy Amplification Property

• Channel Coding with Side Info. (Writing on Dirty Paper)
  – Gaussian noise: No loss.
  – Aperiodic noise: Arbitrarily large loss.

• Source Coding with Side Information (Wyner-Ziv)
  – Gaussian source and squared-error distortion: No loss.
  – Aperiodic source and distortion: Arbitrarily large loss.
Aperiodic Noise

**Definition:** A set $\mathcal{Z} \subset \mathcal{G}$ has **unique differences** if

$$z_1 - z_2 = d$$

has at most one solution for $z_1, z_2 \in \mathcal{Z}$ and $d \neq 0$. Equivalently, if

$$|\mathcal{Z} \cap (\mathcal{Z} + d)| \leq 1, \quad \forall d \neq 0.$$

**Definition:** A random variable $Z$ which is uniformly distributed on a set $\mathcal{Z}$ with unique differences is **aperiodic noise**.

- Autocorrelation of $P_Z$ has minimal upper bound of $1/|\mathcal{Z}|^2$. (Except at zero.)
Difference Sets

Definition: A planar difference set $\mathcal{D} \subset \mathcal{G}_L$ satisfies

$$|\mathcal{D} \cap (\mathcal{D} + g)| = 1, \quad \forall g \neq 0.$$

- Maximal set with unique differences.
- Example: For $\mathcal{D} = \{1, 2, 4\} \subset \mathcal{G}_7$

$$\mathcal{D} + 1 = \{2, 3, 5\}$$
$$\mathcal{D} + 2 = \{3, 4, 6\}$$
$$\mathcal{D} + 3 = \{4, 5, 7\}$$
$$\mathcal{D} + 4 = \{5, 6, 1\}$$
$$\mathcal{D} + 5 = \{6, 7, 2\}$$
$$\mathcal{D} + 6 = \{7, 1, 3\}$$
**Result from Design Theory**

**Lemma:** A planar difference set $\mathcal{D}$ exists with $|\mathcal{D}| = \alpha$ for

$$\alpha = p^m + 1, \ (p \text{ prime, } m \text{ arbitrary integer}).$$

The addition is over mod $L$, where

$$L = \alpha(\alpha - 1) + 1.$$ 

- Can generate from primitive cubic in $\mathbb{F}(p^m)$.
- Example in $\mathcal{G}_{307}$:

$${1, 2, 4, 45, 57, 62, 68, 76, 83, 92, 96, 125, 161, 179, 201, 211, 238, 263}$$
Entropy Amplification Property

**Theorem (EAP):** If $Z$ is aperiodic noise on $\mathcal{Z} \subset \mathcal{G}$ with $|\mathcal{Z}| = \alpha$, and $X$ is any RV on $\mathcal{X} \subset \mathcal{G}$ with $|\mathcal{X}| = \beta \leq \alpha + 1$, then

$$H(X) + H(Z) - \frac{\beta - 1}{\alpha} \leq H(X + Z) \leq H(X) + H(Z).$$

- Lower bound tight for $\mathcal{Z}$ difference set, $X$ uniform on $\mathcal{X} \subseteq \mathcal{Z}$.
- Upper bound asymptotically tight for $X$ uniform on $\mathcal{X} \subseteq -\mathcal{Z}$.

**Corollary:** For any $\epsilon > 0$, there exists a planar difference set $\mathcal{D}$ such that if $X$ and $Z$ are i.i.d. uniform on $\mathcal{D}$, then

$$H(X - Z) - H(X + Z) \geq 1 - \epsilon \text{ bits.}$$
Writing on Dirty Paper

- Two independent additive effects:
  1. “Interference” (S): Known non-causally at encoder.
  2. “Noise” (Z): Not known directly.
- Constrained input (X).
- Coined by Costa in 1983.
Comparison System: Zero-Interference

- Same noise, same input constraint as WDP
- Equivalent to WDP with interference also at decoder
- Could be called “Writing on Clean Paper”

\[ \text{Loss} = C_{ZI} - C_{WDP} \]
Some Prior Results

For real alphabets and power constraint (\( \sum x_i^2 \leq nP \))

- \( S, Z \) Gaussian \( \Rightarrow \) Loss = 0 [Costa ’83]
- \( Z \) Gaussian \( \Rightarrow \) Loss = 0 [Erez-Shamai-Z. ’02, C.-Lapidoth ’02]
- Loss = 0 (for many strategies) \( \Rightarrow \) \( Z \) Gaussian [C.-Lapidoth ’02]
- \( E[Z^2] \leq P \) \( \Rightarrow \) Loss \( \leq \) 1/2 bit [Z. ’02]
Discrete WDP

- All addition mod $L$ with results in $G_L = \{1, \ldots, L\}$.
- Hard input constraint: Each $x_i \in C \subseteq G_L$.
- Strong interference: $S_i \sim \text{Unif}(G_L)$,
  \[ C_{\text{WDP}} = \sup_{P_V, Q(\cdot)} H(V) - H(Q(V) + Z), \]
  where $Q(v) - v \in C$ for all $v$.
- Zero interference:
  \[ C_{\text{ZI}} = \sup_{P_X} H(X + Z) - H(Z), \]
  where $P_X$ has support only on $C$. 
What causes large loss?

Noise must be “non-Gaussian”

- Prior results: No loss $\Leftrightarrow$ Gaussian noise.

Noise must be aperiodic. Consider:

- Noise $Z$ only on $\{\beta, 2\beta, \ldots, L\}$.
- Constraint set $\mathcal{C} = \{1, \ldots, \beta\}$.
- Given $m \in \mathcal{C}$ and current interference $s$,

$$((m - s) \mod \beta + s + Z) \mod \beta = m.$$  

Input: $x \in \mathcal{C}$

Output: $y$

Need “aperiodic” noise...
Capacity with Aperiodic Noise

**Theorem:** For $Z$ aperiodic noise on $\mathcal{Z}$, and any $\mathcal{C}$ with $|\mathcal{C}| \leq |\mathcal{Z}|$.

- With no interference,
  \[ C_{ZI} \geq \log |\mathcal{C}| - 1 \text{ bits/channel use}. \]

- With strong interference,
  \[ C_{WDP} \leq 2 \text{ bits/channel use}. \]

**Implications:**

- Loss at least $\log |\mathcal{C}| - 3$
- Loss can be arbitrarily large
- Loss can be arbitrarily close to 100%
Proof of Capacity Results

Applications of Entropy Amplification Property:

1. Let $X$ be uniform over $\mathcal{C}$,

\[ H(X + Z) - H(Z) \geq H(X) - 1 = \log |\mathcal{C}| - 1. \]

2. Let $K(\cdot)$ re-quantize $Q(V)$ with $|K^{-1}(k)| \leq |\mathcal{Z}|$,

\[ H(V) - H(Q + Z) \leq H(V) - H(Q + Z|K) \leq H(V) - H(Q|K) - H(Z) + 1. \]

Remainder of proof:

- Show $H(V) - H(Q|K) - H(Z) \leq 1$. 
Variation on Wyner-Ziv Source Coding: Compressing an Encrypted Source

- Source $X^n$ and correlated random variable $Y^n$.
- Key $K^n$, independent of $(X^n, Y^n)$.
- Reconstruction $\hat{X}^n$.
  - Must satisfy distortion constraint.
  - Equivalent to reconstructing $X^n + K^n$. 
Comparison System: Key at Encoder

- Same distributions and distortion constraint as before.
- Key does not play a role here.

\[
\text{Loss} = R_{X+K|K,Y}^{WZ}(D) - R_{X+K|K,Y}(D)
\]
Some Prior Results

For real alphabets, squared error distortion ($\sum(\hat{x}_i - x_i)^2 \leq nD$):

- $X, K$ Gaussian ($X$ and $Y$ ind.) $\Rightarrow$ Loss = 0 [Wyner-Ziv ’76].
- General distributions $\Rightarrow$ Loss $\leq 0.5$ bits [Zamir ’96].

For binary alphabets, Hamming distortion:

- Loss $\leq 0.22$ bits [Zamir ’96].
Compressing an Encrypted Aperiodic Source

Consider finite group $\mathcal{G}$, subset $\mathcal{S} \subset \mathcal{G}$ with unique differences.

- Let $K$ be uniformly distributed over $\mathcal{G}$.
- Let
  \[
  X \sim \begin{cases} 
  \text{Unif}(\mathcal{S}), & \text{w.p. } 1 - \epsilon \quad (Y = 1), \\
  \text{Unif}(\mathcal{G}), & \text{w.p. } \epsilon \quad (Y = 2). 
  \end{cases}
  \]
- Let
  \[
  d(x, \hat{x}) = \begin{cases} 
  0, & x - \hat{x} \in \mathcal{S}, \\
  \infty, & x - \hat{x} \notin \mathcal{S}.
  \end{cases}
  \]
Loss for Aperiodic Source

Let $U_S$ and $U'_S$ are i.i.d. uniformly distributed on $S$.

\[
\text{Loss} = (1 - \epsilon) \left[ H(U_S - U'_S) - \log |S| \right] \\
\approx \log |S|.
\]

Tight for $\epsilon$ small and $S$ large difference set (by EAP).

- Loss can be arbitrarily large.
- Loss can be arbitrarily close to 100%.
Conclusions and Future Directions

Main tool: Aperiodic Noise and EAP.

- Generalize EAP to large support.
- Find other uses of entropy amplification.

Main result: 100% loss for WDP and for Wyner-Ziv.

- Extend to real alphabets and average distortion constraints.